HIT Standards Committee
Privacy & Security Workgroup
Transcript
January 11, 2013

MacKenzie Robertson – Office of the National Coordinator
Thank you. Good morning everybody. This is MacKenzie Robertson in the Office of the National Coordinator for Health IT. This is a meeting of the HIT Standards Committee's Privacy & Security Workgroup. This is a public call and there is time for public comment on the agenda. The call is also being recorded so please make sure you identify yourself when speaking. I will now quickly take the roll call. Dixie Baker?

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
I'm here.

MacKenzie Robertson – Office of the National Coordinator
Thanks Dixie. Walter Suarez?

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
I'm here.

MacKenzie Robertson – Office of the National Coordinator
Thanks, Walter. John Blair?

John Blair, III, MD, FACS – Taconic IPA – President
Here,

MacKenzie Robertson – Office of the National Coordinator
Thanks John. Mike Davis?

Mike Davis – Veterans Administration
I'm here.

MacKenzie Robertson – Office of the National Coordinator
Thanks Mike. Tonya Dorsey?

Tonya Dorsey – Blue Cross Blue Shield, South Carolina – Chief Implementation Architect
I'm here.

MacKenzie Robertson – Office of the National Coordinator
Thanks Tonya. Lisa Gallagher? Leslie Kelly Hall?

Leslie Kelly Hall – Healthwise – Senior Vice President
Here.

MacKenzie Robertson – Office of the National Coordinator
Thanks Leslie. Chad Hirsch? Peter Kaufman?

Peter N. Kaufman, MD – DrFirst – Chief Medical Officer and Vice President, Physician IT Services
I'm here.

MacKenzie Robertson – Office of the National Coordinator
Thanks Peter? Ed Larsen? David McCallie?

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
Here.

MacKenzie Robertson – Office of the National Coordinator
Thanks David. John Moehrke?

(Indiscernible)

MacKenzie Robertson – Office of the National Coordinator
Was that you, John?

John Moehrke – GE Healthcare
Yes, I'm here.

MacKenzie Robertson – Office of the National Coordinator
Okay, great. Sharon Terry? And are there any ONC staff members on the line?

Will Phelps – Office of the National Coordinator
Will Phelps. Hi, MacKenzie.

MacKenzie Robertson – Office of the National Coordinator
Hi, Will. And we have Chris Brancato and Charlie Kirby as well. So Dixie, I'll turn it back to you.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Okay. Thank you all very, very much for calling in today. We have only one thing on our agenda today, is to complete crafting responses to the items from the RFC that have been assigned to the Privacy& Security Workgroup. Distributed before the meeting was a document, a Word document, that contained draft responses to the comments we've discussed thus far and I asked you to review those and come prepared to this meeting to submit any comments that you had on those before we start on the remaining items. There are quite a few remaining items. We have two hours and our comments are due to the ONC today. So, we need to move along and between Walter and Charlie Kirby from ONC and myself, we will capture the gist of what we're saying. We won't capture every word, but, we will come…for each item, we will come to a conclusion and I will try to as succinctly as possible, state what we've concluded and then we'll move on. Okay, are there any questions about that?

Okay. Then – so let's start with, are there any questions – are there any comments about the – how we worded the responses, the comments to the, our responses to the first group of items that was assigned to us; in other words, the items that we discussed at the meeting on Monday? Yeah, no? Okay. That's great. But if you do, you know, I will get those into MacKenzie today, so if you think of something after the meeting, jot it down and send it to me, but for the most part, we'll go with what's written there right now. With that, can – Caitlin, can you display the – it's called something like larger copy or something like that. I asked Will and his team to take these comments, and it's exactly what's on the other, what's the other document, but I've noticed in previous meetings that it's literally impossible to read on this screen, so I asked them to make us a larger copy, so that we at least stood a chance of being able to read what it says.

This first one, this is where you'll recall that we had a few that were really specific measures and certification criteria, but now, at this point they're all questions that were directed to us and we were tasked to respond to. Uh huh? Somebody trying to say something?

MacKenzie Robertson – Office of the National Coordinator
I don't think so, Dixie.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Okay, okay, sounded like I was talking over somebody. Okay, for each questions we have the question at the top and then below it, we have the comments that we've received. We've made no attempt to bring these comments together; we've just listed each person's comments with their initials afterwards so that you can see everybody's comments. Okay. The first one is, "What can be included in EHR technology to give providers evidence that a capability was in use during the EHR reporting period for measures that are not percentage based.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
Dixie, this is Walter. Can I jump in …?

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Sure, absolutely.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
Just a quick question on the – did we work through MU04, it looks from the document that captured the revised comments, that MU04, which is those three questions, still has some …

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yeah, you're right. I'm looking at the other document, yeah, yeah, yup. So, let's … good …

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
Should we start with that one first?

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
We absolutely should. Thank you very much.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
Okay.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Thank you very much. So, MU04, and you can find this on the other document and then we'll go to the larger typed copy. MU04 is that some federal and state health information privacy and confidentiality laws establish detailed requirements for obtaining patient consent for sharing these especially sensitive types of information. And this relates to the work that Joy Pritts has been doing in her group on the consent…you know, on the protection of these specially protected types of information like substance abuse and sexually transmitted diseases and mental health, etcetera. And we were asked to answer three questions…and we are the primary on this one as well.

The first one is, "How can EHRs and HIEs manage information that requires patient consent to disclose, so that populations receiving care covered by these laws, these especially sensitive laws, are not excluded from health information exchange?" And then secondly, we'll go through all of them, "How can meaningful use help improve the capacity of EHR infrastructure to record consent, limit the disclosure of this information to those providers and organizations that specified in the consent form, and manage consent expiration and revocation and communicate the limitations of use, and restrictions on re-disclosure?" A very tough problem. The third is, "Are there existing standards, such as those identified by the Data Segmentation for Privacy Initiative implementation guide, that are mature enough to facilitate the exchange of this type of consent information in today's EHRs and HIEs?" So Walter, would you like to start by giving your thoughts on these?

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
Sure, yeah. I guess on the first question about how can EHRs manage information that requires patient consent. My comment on this, the question points to the Data Segmentation for Privacy Initiative of this and a framework. My point, I think there is that while the work being done in this initiative is very promising, I think the overall metadata tagging approach for segmenting and sequestering information is not yet really ready for full adoption through regulations. I think there is more developing, development, specification development, terminology refinement, testing, piloting of the concept, the scalability of that concept across the industry, before it can be fully adopted in terms of a regulation that defines this as a standard and as a certification criteria for EHRs. So, that's my point I think, on the first question.

The second question, I think the – you know, how can meaningful use help improve the capacity of EHR infrastructure to record consent. I think EHRs should have the capability, the capacity, to record electronically consent choices made by the consumer, where those are required to be offered either by some regulation in state or federal levels, or by an organizational policy. But I think there is a risk, of course, of creating the capability and the technical ability to do so in an EHR and then expecting that that will be the requirement across the board. In other words, you know, the capability can and should be developed, but should follow policy, not the other way around. And then the last question, are there existing standards, such as those identified in the data segmentation project, that are mature enough. I think I mentioned that I don't really see those yet, mature enough or tested, developed and tested well enough to be able to be adopted nationally as the standard and the expectation for all EHRs to do and use and follow.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Okay…

Mike Davis – Veterans Administration
This is Mike Davis. I'd like to respond to Walter a little bit.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Uh huh.

Mike Davis – Veterans Administration
So Walter, you know the VA has, you know, been one of the organizations in data segmentation for privacy that's been working in this area and we're heavily engaged in this and in the standards development. And we're in the process of implementing data, various mechanisms for data segmentation right now. So, I would say that we do have an initial set of vocabulary sufficient for data segmentation that has been developed in HL7, but I don't think that – I agree with you that there's a question about the maturity and the ability of EHRs to do this. But some of us, notably the VA and SAMHSA have legal requirements surrounding the protection of these types of data. So, while you could definitely say that the maturity of trying to manage data tagging for the entire range of possible choices is…we're not ready for that yet. There are limited vocabularies that might offer some immediate things, particularly things like…that are driven by the legal laws that we have right now for HIV or sickle cell or drug and alcohol abuse, these kinds of things. So, a very limited set, not to try to take on what HL7 has defined with probably a couple of hundred different data tags.

So, I believe that a limited set is possible, and actually there are two parts of that. One is the ability of the EHR to clinically identify such things, which is not the responsibility of the security system, it's a clinical…purely a clinical responsibility; but then to enforce separation of these kinds of things out is now the responsibility of the security system, which would obviously rely on the clinical tagging. So, a separate security service that, based on rules, could implement privacy consents based on these tags is what we've been demonstrating at HIMS and HL7, and so I don't think it's out of the realm of possibility to say that there are standards that they have been demonstrated that there are organizations, you know, moving towards this, but potentially a very limited set initially would be possible.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Um, thank you…

John Blair, III, MD, FACS – Taconic IPA – President
This is John Blair. Can I make a comment?

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Sure. Hi, John.

John Blair, III, MD, FACS – Taconic IPA – President
Hi. Just a couple, just a question. I wonder if we should be separating the discussion about segmenting and tagging data from the consent management question first.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
That's exactly what I, what my response says and I was getting ready to say, yeah.

John Blair, III, MD, FACS – Taconic IPA – President
Okay, so that's my first point. The second is the consent management, in my mind, resides…the system resides outside of the EHR. I mean, I understand the need for the EHR to record and hold that consent document and be able to have in their software the ability to log that. But it's, I mean, I think of the EHR as interacting with that consent management system outside of the EHR, whether it's NWHIN or HIE or whatever; and if that's the case, doesn't it become more of a question of standardizing the consent management specs that the EHR would deal with. So, my two comments.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
It's, my comment on there is quite long, but it's very similar. It captured a lot of what both Mike and John said. I think that there are two chal – well first of all, I think the way we currently manage both consents and special types of information really, really needs work badly, because I think that what I see so far are a lot of people trying to translate into electronic workflow a broken process to begin with. But I agree with John that the two, the tagging of highly sensitive information is a different thing from the management of overall patient consents. In fact, I think it's very similar to what the DOD, how the DOD differentiates between mandatory access control and identity-based or … based access control. And I think that, and we will capture – Mike has made an important point that there is a limited set of vocabulary that could be used for tagging these special types of information and we do have preliminary work in that area. And I agree that we need both the ability for the EHR to identify and respond to these sensitivity tags, and we need the ability of the EHR to manage consent and enforce security according to the rules that are based on both.

M
This is …

Mike Davis – Veterans Administration
… just recently captured this quite well and I think you'll find broad agreement on this. I've been talking with the EHR group in HL7 and I think they would concur that there are two facets; one is purely the clinical side, the tagging of clinical fact, I mean, if a person has an HIV or not, that's a clinical fact. There's no bias, prejudice, or anything about it, you either do or you don't. The security system, on the other hand, is looking at this from a different perspective. The potential for embarrassment or compliance with a legal thing and it's all about the risk, the perceived risk even, of exposure of this information having some type of negative effect, and these are policy matters, outside of the cold, analytical portion of the EHR, that the security and privacy people deal with, and these perceptions change over time. What we need to start with is the clinical vocabularies to define these, and I think they're there, whether all EHRs actually implement this is a different question, but I think the vocabularies on the clinical side are there. And then the mapping of those to a set of privacy and security attributes that reflect the policies is a different matter.

John Moehrke – GE Healthcare
This is John Moehrke.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Uh huh.

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
And David McCallie, I'd like to chime in after John.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Okay, John.

John Moehrke – GE Healthcare
So, I did submit, you know, actually I think probably my longest comment is on this particular one and it very much mirrors what's been said, so I'm not necessarily going to repeat that. To get more towards well what could we say, I think when you look at how sensitive data is managed, and who or what system makes the decisions about whether information gets disclosed or not, and what information about the request or the requestor is needed in order to make those decisions. Much of that is the space that's…you know, that Mike has been really exposing quite nicely in his demonstrations of data segmentation for privacy and when we look at that, it is not far from what the requirements were that were put into the secure SOAP stack, which is part of Meaningful Use Stage 2. The criteria that are in that specification already in Meaningful Use Stage 2, carry with it user identities and their roles and the purpose of use and that's the critical information that a responding system, a system holding information and holding rules about disclosure of that information need in order to say "yes" or "no," that this information needs to flow. In addition, the tagging that would need to identify this piece of information as normal clinical information versus this information being restricted information is also a part of those specifications.

So, I think we can actually have some positive in that there are some stepping stones, some current technology that's already been selected by meaningful use, but there is some functionality that needs to be implemented in order to make it work. You can't just simply say, yes, I've identified the user in the system and the purpose of use and all that, and magic happens. The rules of engagement need to be understood, and I think that's not in certification space, that's more in actually space above HHS, in the privacy regulations, are very confusing to come down on what are the rules that you need to engage. So again, that gets above our needs.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Okay.

John Moehrke – GE Healthcare
So, I think we do have some stuff already in play and I think we need to expose that it's there to be used and this is how you would use it.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Now you mentioned the SOAP stack for Meaningful Use Stage 2, I assume you're talking about the exchange specification for transport.

John Moehrke – GE Healthcare
Correct.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
What – it just addressed the discretionary control – does it address both the mandatory and discretionary controls?

John Moehrke – GE Healthcare
It does not, again, whether you're going discretionary or mandatory, that is architecture of the access control decision and … transport …

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
What I meant, I meant by – does it address both tagging and individual consent is what I should put it?

John Moehrke – GE Healthcare
It addresses user identification and it does address a high level tagging confidentiality code. It does not address sensitivity code, so, it does not have the ability today, and this is some of the extensions that Mike has done in data segmentation for privacy, does not have today a way to carry what is the sensitivity reason, but it does have a way to carry what is the confidentiality code.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
So that's what you mean by stepping stone, it's already the ba-, the foundation is in meaningful use. Okay, yeah …

John Moehrke – GE Healthcare
The foundation is there.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Got it. David?

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
Yeah, this is David, can you hear me okay?

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yes.

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
Good. I am sort of generally in agreement with what's been said, but with a couple of caveats and concerns. The broad context is that I think we should encourage ONC to experiment with simple and straightforward use cases and see how well we can make that scale before we try to jump into the really complicated use cases. And so one of the simple use cases that we started talking about on the Tiger Team call a week ago, I think you were on the call …

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Um hmm.

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
… which is certainly not a finished thought, but it got some traction and I think it has some potential for becoming an organizing concept, is this notion that we crafted called directed query, where you explicitly account for the common use case of where the patient is with the current provider and he authorizes that current provider to request data from some previous source; and it could be in this case a restricted source. And what I would encourage us to suggest is that we optimize for this common use case where the patient…where we find a mechanism, technical and secure mechanism to allow the patient to assert that he wishes the data to be released at this point in time to this particular provider for his ongoing care. And if we can make that use case work, particularly for the sensitive data that would not otherwise normally be released, I think we get a stepping stone, to pick up on the stepping stone metaphor, a stepping stone to more complicated indirect care cases where the patient isn't in the loop as the direct authorizing authority.

So I like the piloting work that Mike and the VA are doing and I like the refinement of the vocabularies that HL7 is doing and the understanding of what does and doesn't work with the SOAP stack, in terms of what kinds of information is captured. But I would urge us to put this focus on this very simple use case of directed query, when the patient says, I authorize you as my treating physician, to have access to this data from this remote site, which might contain sensitive data. And here's an assertion that can be communicated in a trusted framework, in a technical way, so that the releasing system has a "safe harbor" and I don't mean that necessarily legally, but the spirit of a safe harbor, to know that it's okay to release that data. And if we can't make that work, then I think we are unwise to go to more complicated systems.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Well I don't think that that's all that easy because I think that, as I've expressed before, you've heard me before, because the...having a patient with the requestor saying, "Go get this data," and then that's the consent that they're giving to the requestor, not a consent that they're giving to the holder of the data, which might, which most likely has a different consent.

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
So how could the patient …

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
I don't think that's the simplest case, and I think that the whole system needs to be looked at in terms of all of these exchanges where the consents reside, you know, currently, consents reside locally and you've come into exactly those kinds of difficult …

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
Well how – Dixie, I don't understand. If the patient isn't able to allow his data to be released, how can the data ever be released?

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
He can, but he needs to provide that consent to the holder of the data…

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
… idea, that's what I'm suggesting, is the technical protocol by which the patient could provide that consent to release the data to the holder.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
To the holder…okay, okay.

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
(Indiscernible)

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yeah, I thought you said, I thought, I've always thought when you bring this up, that you're, they're sending some document over and the doctor goes, you know, Dixie was in here today and she said that you can send me her data, you know? If there's a mechanism where a patient can remotely update their consent in a trusted way, I think that that's definitely needed.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
Yeah, I mean this is …

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
So let me finish and respond to Dixie just a second, because I think that technically that's exactly what I'm saying, the patient tends a consent for release, I'm just saying that that happens built into the physicians query or we make systems such that that could happen built into the physicians query, while the patient is there. In other words, we don't require that the patient be … place to declare that the data should be released, and then go see the doctor and say, "See if you can get it now." I mean, you could do it that way and I have no objections to that, of course, but why not just say when you're with a physician and he says, "I see that you've received care at the VA, will you give me permission to release those sensitive records," and the patient says "yes" or "no." If that information could be securely trusted and transmitted, then the system would work when it's needed at the point of care.

Now, he could get a standing order that says, "I always want it released to Dr. Smith," or he could give a standing denial, but we should operate – we should be able to at least account for the common case, where the patient is right there, to be seen that day, authorizes the release, the data gets pulled and can go forward.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
So I see, I agree we need to address that use case. I totally agree. I don't think on this call we're going to resolve it, but I totally agree we need to address that use case, yes.

John Moehrke – GE Healthcare
This is John, just one quick comment. This is a reality check. I think that all makes sense. It's probably not practical in day-to-day care for the physician to do that. I don't think they'll begin, come close to taking the time to do that. So, in the workflow, it's got to be some proxy …

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
John, the way it really works in most cases is, you know, whenever there is a patient that is going to be seen by say a specialist, and the specialist needs to receive the data from the primary care provider referring the patient, the specialist would request the data, or would request that the patient authorize the specialist to request the data. And they will send that to the primary care physician and the primary care physician will have mechanisms to verify the identity and the trust of the specialist that is requesting that data and they will make a decision at that point of saying well, I need the patient to actually sign and send me a document on my letterhead that authorizes me to disclose that data to the specialist. That's one path. The other one is saying, well, I accept the form that you specialist sent me to, signed by the patient, to disclose the data to you, and I will keep that as a very, you know, a legal document that authorizes me to disclose the data to you. So those are the two paths that would happen, sort of in real life actually.

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
I'm not arguing …

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Hey, we only have two hours and we have a lot of questions. I think we have very clearly concluded unanimously, that this is an area that needs a lot of work and that it should start with common use cases, work them through. And it should address … and we need a solution that addresses both the labeling of sensitive, of information that's sensitive based on – it's medically sensitive and we also need a solution for managing individual consent. And we need a solution that puts all this together and that that solution is likely not to replicate what happens on paper. Everybody…

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
So Dixie, here's what I ….
Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Would everybody be happy with that kind of re – we can't spend an hour on this, we can't spend …

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
So here are the four points that summarize what we just said. Number one, EHR to be able to electronically capture, maintain and report consent choices and that's confirming that that should be a capability that EHRs should have. Number two, there are a limited number of confidentiality and sensitivity codes that have been tested and can be identified for use, that's the point that Mike made. Number three, there are, there is a need to test use cases that demonstrate the scalability of an approach to address consent management. Number four, there needs to be a more widely tested approach to a more comprehensive consent management process itself, because there are elements of consent management that do reside inside the EHR and then there are elements of consent management that reside outside of the EHR.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
So we're not talking about – I agree with the points except we're not talking just about consent management. These are two different problems …

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
No, I'm addressing the both of them.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
They have to converge in that mediation activity and that decision making of whether to release the data or not, they must converge, but they're two separate things; one based on law and medical fact and the other based on … consent is based on an individual's permission.

Peter N. Kaufman, MD – DrFirst – Chief Medical Officer and Vice President, Physician IT Services
This is Peter, can I make two quick points, because I know we want to move on. One is, this is a point that was brought up by Blue Cross of Massachusetts about ten years ago, we do want to get this past the point where the patients are not feeling threatened and we may need to make some compromises in terms of the ease of consent, in terms of getting patients more comfortable with it. Better that we should have the patients feeling comfortable with this and a little more work for the doctors, and I am a practicing physician; and then gradually work to making it easier and more straightforward as the patients accept it, rather than having people take it to court and fight it and say they don't want to do anything like this. And then the second point is, I did have a patient one time who came in and asked me not to talk the referring doctor, and it turned out, and this was back in the days when it was a death sentence that he had AIDS, and didn't want me to know that he had AIDS, and it totally changed the care that he would have gotten, and I didn't find out until he had actually committed suicide, about what was going on with him. And we need some, at least to keep in the back of our minds, some way of getting past that kind of a factor, although it may be a second stage. And now I'll be quiet.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Thank you.

Mike Davis – Veterans Administration
This is Mike. I agree with Dixie, we need to move on and I think she's captured all the points quite well. I think we're kind of designing this now. The intent, I think, it's not scalable to have clinicians involved in this with patients and it certainly is possible to say that, but …

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
Mike, I want to object just a little bit, that in the real world today with Surescripts, this is exactly the model that is used, but the clinician doesn't do the work of capturing permission, that's done in the front office …

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
We do need to move on David. You know I don't like to cut people off, but we absolutely need to move on. Please display the next question. Okay thank you, thank you. Now we stand a chance, not a big change but, okay, this one has to do with giving providers evidence that a capability was in use during the EHR reporting period, for measures that are not percentage based. This capability needs to support measures that occur at all stages of meaningful use. So, are there objectives and measures – so they're really asking on the objectives and measures side, they're not asking us about standards at this point, that should be prioritized to help providers show that they've used a particular capability during a reporting period. Walter?

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
Yeah, I didn't actually identify to the last part of the question, the objectives and measures that should be prioritized. My only comment was that certainly there is a possibility that the EHR audit trail process and methodology is used monitor and document and demonstrate that a particular capability that is required in the meaningful use is indeed sort of turned on or activated during the reporting period. So I do think that the audit trail…EHR audit trail process and standard and technology and methodologies would allow to do that. I didn't document here examples of … for those measures that are attestation measures, not percentage measures, which ones could be done through, which ones could be documented as being indeed turned on or activated as a capability, using audit trail, but I do believe that there is that ability to do it using the EHR audit trail capability.

Leslie Kelly Hall – Healthwise – Senior Vice President
This is Leslie. Walter, I think the concern is that some vendors are being certified with a product, installing a certified product, but not necessarily the client is getting delivered those features in the way that was indicated in the certification. So, if the audit trail can capture it back to those specific features, I think that's exactly the right approach.

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
Wait a minute, this is David. Are you – I'm not sure that's what – I thought this was just to facilitate the measurement of the use of the feature, not to prove that it was implemented properly.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yeah, that's what – I think that is what it is. You know, the problem that I had with this one is that yeah, audit will tell whether it's used or not, but at what point to you really start interfering with the delivery of care if you've got all of these things that are overlooking. You know, it almost becomes stalking, of what the provider is doing. I'm not sure what they're trying to get here. David, do you know more about that?

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
I think it's what's done today in an ad hoc way by the vendors, where these are …

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
I think you probably have your headset, can you adjust it a little bit, you're coming in …

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
Okay, I'm sorry, is that better?

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yes, it is. Thank you.

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
Okay. I think it's what EHR vendors do today in an ad hoc way by generating reports that allow our clients to easily summarize the use of a particular feature. So, you know, how many patients had an order placed via CPOE during this encounter. Well, we can run a report to come up with that number. So I think …

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
But David, don't you, but don't, I mean, my sense, don't you think that the question is really not about the measures that are percentage based measures, because those percentage based measures, we as providers have to document and demonstrate…and be ready to demonstrate those. So, those are not the concern. I think the concern are those …

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yes.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
… attestation measures, measures that are just known, in which my CFO signs a letter saying, I attest that we do have that capability. But then when it comes to a "kind of external audit" by CMS saying, you know, show me that you are indeed activating this capability, or that the EHR has that capability activated that gives you the evidence that you say "yes" I am attesting that we are doing that. I think that's what this is about and that's what I was trying to point out that the audit trail of the EHR should be …

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
I think that's good Walter, and that's a good clarification, but, my question then would be, what does "in use during the reporting period" mean, and how would you capture that in an audit trail? Does it mean in use for a percentage of time, that it was in use at least once, that it was never turned off…

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yeah, I see what you're saying. Yeah, you're saying…you're agreeing that we're talking about measures that are currently attestation and if you use audit and they use it once, does that prove their attestation…

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
Yeah, and, I mean, what I would really strongly assert is that it's unlikely that we could develop a standard way to do this. Now, it might be the case that you required a vendor to have for each attestation measure some way to do it, but, I'm…I think it's unlikely that we could come up with a generic and standard way to do it, given the vast differences in the way people implement each capability.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Well do they think – what's the problem that they're trying to address here? Do they think that people are attesting and lying about it or…

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
Yes.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
Yeah, I mean…

Leslie Kelly Hall – Healthwise – Senior Vice President
Or that the vendor has turned off the feature and the patie – how does the provider know that they're attesting to something that a feature exists and defined in the standard.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
There are two sides, it's whether the EHR that was certified when it was installed, the EHR does have that capability indeed. And number two, whether the provider that is attesting did actually activate the capability. So, it's both ends, it's sort of the EHR vendor side of confirming that the certification that says that they have the capability for that attestation measure does get installed if you will, in the EHR of the provider. And then on the provider end, that the provider has actually activated that measure that they are attesting for.

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
And it could, there's, do any good examples come to your mind, Walter?

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
I was going to pull out a couple of the attestation measures just to give, but I'm having trouble with my computer right now. But yeah, I think that would be the way to look at this, is take one or two attestation measures and say, how can the EHR audit trail, or some other mechanism, help document the fact that the measure was indeed turned on.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Well, if you were – if what you say is true Walter, then by auditing, you wouldn't have to have a percentage, you would have to have just once – to prove that it was there and activated, right?

Leslie Kelly Hall – Healthwise – Senior Vice President
Right, you could have an audit rather than by individual transaction, is this feature on now, is this feature still on now. I mean, I think your point Dixie is you don't want to get so prescriptive that we end up being ... the cost and the time to oversee becomes more than the value of the feature.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yes, yes.

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
Exactly. I agree totally with Leslie…

M
I do too.

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
... that it could become overbearing.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yeah, that's what I – that was my impression when I read this.

M
I'd like to make just one point is that as a security person, I'd remind that the audit system is a security system and it's for security purposes and not administrative purposes, although that's a battle that I continuously tend to lose, so …

Leslie Kelly Hall – Healthwise – Senior Vice President
Although the same thing could be said for any…

M
… journaling is correct, but you know, but already turning off audit systems …

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Leslie, wait a minute…

M
… because they're overburdening the basic functionality of the system. And now you're going to, you're suggesting that, if this is the security audit trail you're talking about, we put administrative stuff on top of the actual security stuff it's supposed to be doing.

Leslie Kelly Hall – Healthwise – Senior Vice President
Okay, so I think they are two different things. You've got the audit trail for security purposes that you're talking about and then you just have reporting capabilities that I think Walter mentioned, that said, how do we report that these things are on, these features are on and in use period. So, I don't think they're – it's an overburden of anything for that.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Well, an audit trail, a security audit trail would know that something was on, whether it was on or not. You wouldn't have to collect any additional data, it would show that. It's just that you would have to have somebody look at it to see that it showed that. So, what do we want to say here? Do we want to say – Walter has suggested using audit trails?

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
I would say maybe, that we'd just suggest that this would have to be taken on a case-by-case basis. It sounds like I'm really causing a lot of static …

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
You are, yeah.

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
I'm not sure why. Taken on a case-by-case basis. In some of the cases, there may be a utility for, a use for an audit trail, but not in all cases, but in every case, we should make sure that we're not overburdening the system and the system administration for little or no benefit.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
So on a case-by-case basis…

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
So here's one very specific example, implement drug-drug and drug allergy interaction checks. That is not a numerator denominator measure; it is a just no answer measure, an attestation. So the EP has enabled this functionality for the entire EHR reporting period, it's the measure. And the attestation is basically a signature that says, "Yes, we have enabled that functionality for the entire period." And what this is attempting to do is, are there ways by which through some collection of information automatically, not manually because that's what would have to be done today to demonstrate that, is there a way to help the EP document electronically, automatically that the drug-drug, drug allergy interaction check was enabled.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
So when David, when you say case by case, what you mean is looking at the attestation measures on a case by case basis, right?

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
Yeah…

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Looking at each attestation measure, figure out whether the audit trail will do the job or not, and in every case, make sure that whatever mechanism is used, you're not overburdening the system.

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
Yeah, and I can imagine the kinds of complexity that could emerge that would go from the spirit of the law to the letter of the law and cause more harm than good. So for example, let's say, take that drug-drug interaction. You know, what if it's turned on and it's working and there's a bug and they turn it off because there are some dangerous false positives and it's off for a day while the vendor fixes it, then they turn it back on for the rest of the reporting period. I assume most people would asset that in fact the system was turned on during the reporting period, but an audit log that showed there was a gap of twenty-four hours, what would that mean and that now raises all these questions, were you really talking about what percentage of the time was it turned on. I mean, it just…it adds so much complexity for so little benefit. This is simplifying the life of the auditors and I don't think that's what business, the Stimulus Act, is aimed at.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yeah.

M
I think we're making it too hard. If you open up like Windows task manager, you can find some services that have been turned on, and …

Leslie Kelly Hall – Healthwise – Senior Vice President
Only those that are feature …

M
… the system functions …

Leslie Kelly Hall – Healthwise – Senior Vice President
… recognizes.

M
Well, if you're not going to recognize something, add it to the list.

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
But now you … but didn't say you have to keep a record of that for the number of years post that you could be audited, and if so, what format do you keep that record in and who has access to that format and how do you ensure that it hasn't been tampered with and – I mean, it just opens the door to a lot of…

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Why don't we just simply say that the current audit capability has the ability to do this; however, we question – we, let's see, caution that using it in this way does run the risk of overburdening the system while providing little to no value.

Leslie Kelly Hall – Healthwise – Senior Vice President
Well what if it's not the responsibility of the provider, but of the certification, that we state in the certification requirement, not only can you certify that you do it, but you attest that this feature will be enabled for all clients attesting to meaningful use.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Well you can't do that because they're two different, they test the product …

Leslie Kelly Hall – Healthwise – Senior Vice President
Right.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
The attestation is the provider attesting that they have it configured and that they're using it …

Leslie Kelly Hall – Healthwise – Senior Vice President
Right.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
… what … do in the operational environment? So you can't tell a vendor, you know, can you attest that your customers are using this.

Leslie Kelly Hall – Healthwise – Senior Vice President
But you can say that it's turned on, a feature turned on. I…

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Well you can't say that either because, you know, you sell them a product and it's up to the buyer whether they turn it on or not.

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
I think there may be legitimate times when it has to be turned off, like I said, for, you know if there's a bug, for a safety feature. But that doesn't violate the spirit of what meaningful use is; if you've got your drug-drug interaction running 98% of the time, then I think you qualify.

Leslie Kelly Hall – Healthwise – Senior Vice President
I agree its material; it's what's relevant versus the actual detail of a specific percentage or audit.

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
Yes, yes.

Leslie Kelly Hall – Healthwise – Senior Vice President
This is reasonable, we do the reasonable test, which is, this has been turned on and it is used during the attestation period.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
And that's what it is now; they attest that it's used.

Leslie Kelly Hall – Healthwise – Senior Vice President
The issue is that…

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Maybe what …

Leslie Kelly Hall – Healthwise – Senior Vice President
… the problem that I think is trying to be solved, or at least our experience has been, a vendor can attest or a vendor can certify a particular feature, but turn it off.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
No, the user would turn it "on" or "off." Or are you thinking about the defaults when the product is delivered?

Leslie Kelly Hall – Healthwise – Senior Vice President
Yes, or certifying that this product is used, but then how is it…

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
You can't certify if a product is used…or a feature is used. Certification is on the product…

Leslie Kelly Hall – Healthwise – Senior Vice President
Right.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
… and on the usage side, you're doing the attestation or the measurement and it's up to the buyer of the product.

Leslie Kelly Hall – Healthwise – Senior Vice President

So the problem is for the buyer beware problem I think is trying to be solved, is, how do I know that when the product is certified and it's delivered to me, I'm doing this in the way that is indicated appropriate by meaningful use. That's one … right.

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
That might be, but I think they're going after making the auditor's life easier.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
Yeah, I agree with David. I think this is about when a…well, making the auditor's life easier or making the provider's life easier when responding to an auditor request for documentation, I think. That could be another way of looking at it.

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
Yeah, yeah, good point.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Or maybe they just don't trust the attestation. But look at what they…we have written on the screen, and we can clean this up later, we aren't wordsmithing here. But see if that has captured the essence or if there are additional points, and again, make sure – don't get into the wordsmithing, but make sure we've gotten the key points here.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
Yeah, I think this offers no … direction, but the priority idea of saying, since they are asking which priority measures should be looked at, well, those attestation measures for which there is an easy way to use the audit trail capability to document, would be the priority ones.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yeah, that's a good point. Give priority to those attestation measures where the audit trail can actually be used for this purpose.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
Exactly, without overburdening the audit trail system …

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yeah.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
… the audit system, yeah.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Well I don't think you'd have to – yeah, without auditing additional factors.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
Yeah.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yes, or events, yeah.

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
I'd like to add, it will raise the question of what the technical definition of end-use means, but they probably already know that, so ... in continuous use or majority of the time use or whatever.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yeah. We can fix…okay. Give priority to attestation measures where audit trails can be...perfect. Okay, and we can wordsmith it later. Let's go to the next one. Thank you all. Let's go to the next one. Okay, this one is from the Privacy and Security Tiger Team, how can the Health Information Technology Policy Committee's recommendation be reconciled with the NSTIC approach to identification, which strongly encourages the reuse of third party credentials. I think they're referring to something right above that, right. Can you scroll down a bit? Yeah, right there, in this introduction. They refer to the recommendation to accept that EHRs should be able to accept two factors or higher, two factor authentication, for providers and that, let's see – need multiple factors – yeah, they're just talking about their decision to require that EHRs be able to handle multifactor authentication. Then, let's go to their question. The question is, "how can this recommendation for EHRs to handle multifactor authentication be reconciled with the NSTIC approach to identification which strongly encourages the re-use of third party credentials? So …

Leslie Kelly Hall – Healthwise – Senior Vice President
This is, I think, somewhat confusing because it's talking about the identity management, right, the level of assurance that's looking at LOA2/LOA3 and then back to factor authentication, which is a different issue. So, I'm a bit confused, can you clarify that a little bit.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
I think they're talking about authentication, not identity …

Leslie Kelly Hall – Healthwise – Senior Vice President
So but their approach to identity is … identification is then…is that identity or…

Peter N. Kaufman, MD – DrFirst – Chief Medical Officer and Vice President, Physician IT Services
This is Peter. I think I can answer your question. Basically, to get an identity that is a scalable format, you have to go through identity proofing and generally, for medicine for providers it's been considered a NIST level 3 for medical providers identity proofing. And when you've been identity proofed to go to utilize that is to receive a credential that can then be used to say that you were identity proofed. The idea is that that credential, whether it's online or accessed online through a two-factor authentication or accessed directly through a two-factor authentication and using the public key, private key or however you're doing it, you shouldn't need a separate credential to show that you're…for authentication for each different system. So if it's a doctor that goes into practice and also moonlights and goes to three different hospitals, they shouldn't have five different credentials, they should have one that could be reused. And that's the whole point about this is having a trusted credential that could be…once you have one credential, then it could be shared and that's the whole idea behind NSTIC.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yeah, this is …

Leslie Kelly Hall – Healthwise – Senior Vice President
Thank you.

(Indiscernible)

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
… about authentication, it's not about identity proofing, per se.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy

But it seems like the argument they're making is that the HIT Policy Committee recommendation is in some way in conflict with the NSTIC reuse of third party credentials and the argument I make in my comment anyway is that the two are not incompatible, they are complimentary.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Complimentary, I agree. John, why don't you talk about your feedback you provided.

John Moehrke – GE Healthcare
Well yeah, I think I agree with what you were saying, I don't think that there's a conflict indeed, I think NSTIC is showing that there doesn't need to be a conflict. But, I put into my comment that whether you accept a credential or not is a policy choice, it's not really a technology choice, and I think much of the benefit that NSTIC will have is not really going to be ready in time to fold into MU3, which is basically the conclusion. I think it's probably further out there. I certainly would keep an eye on it; I am personally keeping an eye on it. So, I like it, but …

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yeah…

Leslie Kelly Hall – Healthwise – Senior Vice President
This is Leslie. Is that the case, because isn't this for physicians who are doing e-prescribing today, aren't they all – isn't there already the use of an equivalent or this approach specifically and…

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
… he's saying NSTIC is out there, they can…

John Moehrke – GE Healthcare
Yeah …

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
… implement two-factor authentication sooner, but NSTIC is farther out there.

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
The DEA's … is not NSTIC, at least not yet.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
… to what?

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
The DEA model is not an NSTIC protocol at this point. It might become one someday, so, it's two-factor, but it's not NSTIC.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yeah, why don't we capture John's point that, well, there are several points. The point that Walter made that there's no conflict here, in fact, it's complimentary, these are complimentary; the Tiger Team's decision and NSTIC are complimentary. John's point that the decision of whether a provider accepts NSTIC will always be a policy decision, not a technology decision. And the point that they could…we could require two-factor authentication sooner than and in anticipation of NSTIC and they can implement two-factor authentication independent of NSTIC and then use NSTIC when it becomes available. And I think those points will have that question covered. Do you guys agree?

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
This is David. That sounds pretty good to me. I like what John wrote, I think that's quite good.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yeah, I do, too.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
There's another point that both John and I make which is that the idea that implementing NSTIC by Meaningful Use Stage 3 might be too soon, or too risky. But, I know that's not part of the question that we've been asked necessarily, but I think it might be a point worth noting.

Mike Davis – Veterans Administration
This is Mike. Again, Walter, I'm not sure that I agree with that point either. The, we've already … organizations have already implemented federation types, authentication federation services and, you know, I know one particular large organization that accepts both internal credentials and credentials from outside of other organizations and they're managed through a federation service.

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
But Mike, we're not saying that you couldn't do that, we're just saying that it's not NSTIC yet.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yeah,

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
I mean, I think two-party, trusted third-party credentials is the requirement for DEA and many other things…

M
Right…

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Why don't we incorporate that in that sec, third sentence; can, we can require, not request, we can require two-factor authentication or third-party authentication in anticipation of NSTIC. So, those could be required earlier than when NSTIC is actually available.

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
Well I would say – yeah, and the question will be, at some point what we'd hope for is standardization so that your credential would work with any of the EHRs that you have to interact with in your day's work, which as … pointed out, could be multiple different EHRs in different facilities. But the standards to do that are settled enough to bake into certification in time for Meaningful Use 3.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
That's right, good…

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
And it's case by case, unfortunately. That's what NSTIC is going to solve for us, we hope, but like John, I'm skeptical that it will be done in time for Stage 3 certification. By the time Stage 3 is actually deployed, it may be well established, but that's many years after certification software gets written.

Leslie Kelly Hall – Healthwise – Senior Vice President
And it's such a shame because this is such an opportunity for providers to save a whole heck of a lot of money that they spend right now in managing credentials and managing passwords and managing access.

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
Absolutely.

Leslie Kelly Hall – Healthwise – Senior Vice President
It's a crazy amount of money they spend on this today.

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
And just … factor.

John Moehrke – GE Healthcare
I think this is especially – you know, I would like to see it applied first to patient's identity, enabling the patients to access their electronic health information; that's far more the low-hanging fruit because a) … and b) it's likely patients want to use an Internet-based identity.

Leslie Kelly Hall – Healthwise – Senior Vice President
I think it's worth comments because, even though it may not be ready for Meaningful Use 3, that idea of making sure we include the patient in this is going to be very important.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Why don't we simply say that NSTIC offers benefit for both patient authentication and provider authentication and that the regulation shouldn't force the two to progress at the same … in tandem?

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
… we can add that, you know, it should be road mapped into the future stage column, if you will, so that it clearly gives the direction that that's where we're going.

John Moehrke – GE Healthcare
Right.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Okay. Let me see what we have here – we've captured … I don't know if my … is active. Okay, let's go to … for those of you who say … never freeze up, they do. Let's go to the next question please.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
Just Dixie on this one I would just make the point about the future stage and we can wordsmith it later, but …

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yeah, I can't see what's there because I've got to reboot my system, but let's go to the next question.

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
Which question are we on now, is this the 03?

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
02.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
O2.

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
… 02, okay.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Would you read it please? I don't have it up.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
Sure. How would ONC test the HIT Policy Committee's recommendation in certification criteria?

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
How would what?

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
How would ONC test the Policy Committee's recommendation in certification criteria? I suppose this is linked to the previous question about two-factor authentication and all those things. So, how can it be tested in certification criteria?

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
And this is – Walter, do you assume that they mean at NSTIC's approach, in which case wouldn't NSTIC include different testing methodologies?

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Well, it would – in my opinion, and I think I put this on there that, it would be tested just like anything else that's a requirement. You know, NSTIC would be treated just like any other standard that goes through the testing, you know, through scenario testing, etcetera. I didn't understand … why it would be a … why they see it as a special case.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
I think the question was about, HIT Policy Committee recommended use of two-factor authentication or higher and so then, without going all the way to NSTIC, just to that level of simply two-factor authentication, how would or what kind of certification criteria can be developed to test that an EHR is able to handle two-factor authentication.

John Moehrke – GE Healthcare
This is John Moehrke. I think what's unfortunate here is that if indeed NSTIC was in the maturity that it could be included in certification criteria, NSTIC itself, part of their goal is to have certifying mechanisms. So, that's one of the benefits of saying yes use NSTIC is, you know, you would be using their certification functionality. But the maturity problem that we just got done discussing, it's just not going to be ready. So I think once…one of the problems with saying, hey, you could require two-factor authentication and support for federated identity without doing NSTIC, is that you create a need to create certifying technology; whereas if NSTIC was done, you could just say, you know, certified by NSTIC. So, this is a case where the maturity of the NSTIC and really the technology and the deployment of that technology is just a little bit out further than MU3.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
But meanwhile, meanwhile, if you wanted to test just be able, the ability to accept two-factor authentication, you would need to test and write scenarios to prove that the system configured to require two-factors under specified and … conditions and then the ability to detect those conditions. So, I think it's important to … both how you would test, you know, two-factor authentication, and then, once NSTIC then add that … be able to accept NSTIC certification as part of EHR certification; if they're asking for both.

John Moehrke – GE Healthcare
Yeah, the problem is that of course the concept of multiple-factor authentication is in the functional space, it's not in any technical interoperability space. So, you know, there isn't a technical stock that says, this is how you would test two-factor authentication. It's well, if you're using a token and a pass phrase, this is how you would test it. If you're using a cell phone and a … you know, it's only where you …

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yeah, you have to …

John Moehrke – GE Healthcare
… the test has to be specific to the factor system that you chose.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yeah, it does, it does.

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
But Dixie, this is David. Given that this seems to be in the context of the NSTIC question, I think John's answer is right on, is that NSTIC will include certification methodology, that's part of what they're going to deliver and it's just not ready yet.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
Yeah.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yeah.

Leslie Kelly Hall – Healthwise – Senior Vice President
This is Leslie. Is there something that we can do to encourage rapid movement because there are so many dependent on NSTIC moving faster and it seems to be politically acceptable to say, yeah, they're not moving very fast and it's never going to get done. What can we do to encourage this effort to move at a faster pace?

John Moehrke – GE Healthcare
I think you'd have to clone a lot of subject matter experts.

Leslie Kelly Hall – Healthwise – Senior Vice President
Just that?

Mike Davis – Veterans Administration
I think that John's approach would be very good in encouraging this by putting the market to work on patients and not clinicians.

John Moehrke – GE Healthcare
Yeah, focus.

Mike Davis – Veterans Administration
That's right, the commercial use of NSTIC is on customers and that space and we add more customers to that space, it's going to help encourage the development.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
So who would we be encouraging ONC to do something?

Leslie Kelly Hall – Healthwise – Senior Vice President
Encourage ONC to seek rapid cycle development for consumer and patient integration.

John Moehrke – GE Healthcare
Yeah, and I think the method that you do is exactly as Mike said. We need to provide NSTIC a reasonable set of prioritized use cases, rather than say, please solve world hunger in the area of Internet identity.

Leslie Kelly Hall – Healthwise – Senior Vice President
And I think the use cases as defined can be looked at at the ABBI Project for patients …

John Moehrke – GE Healthcare
ABBI would be great.

Leslie Kelly Hall – Healthwise – Senior Vice President
And I think that would keep the use case narrow and then future development would be patient generated health data and how to input data back up into the record would be a separate use case.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
We don't have to come up with a list of use cases, but let's capture the two points that John's made here. The one, to accept NSTIC certification when it's available … why don't you say … why don't you articulate them John, that one and the one that providing NSTIC the reasonable set of use cases. Accept – I think you just said to accept NSTIC … ability to accept NSTIC certification as part of EHR certification is the first point.

John Moehrke – GE Healthcare
I presume you'll wordsmith this offline, right?

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yeah, yeah.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
Well I think the point was that NSTIC provides the certification and so, you know, we should accept that, we should use that certification.
Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yes.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
Then the concern is that we need to encourage moving NSTIC adoption and actual happening faster.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yes.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
And in order to do that, one way is to provide reasonable use cases.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Um hmm. Oh, that's good, yeah, yeah. And the second one, capture both of those points as Walter had done, that encourage ONC to support rapid development of the NSTIC by providing NSTIC with reasonable set of use cases in health, for both providers and consumers.

John Moehrke – GE Healthcare
Reasonable set of prioritized use cases.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Prioritized, yeah.

John Moehrke – GE Healthcare
Otherwise, you would just end up with this flat list … you don't really …

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Reasonable set of prioritized use cases for consumers and providers. Okay, got it.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
We have like four more to go, I think, or five …

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yeah, I know, I know. We've got it. We don't have to wordsmith, that's good, that's good. Let's go to the next one. Okay, the next – I hope they get easier. Should ONC permit certification of an EHR as a stand-alone or an EHR along with a third party authentication service provider? Okay, Walter.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
Yes and then we need clear use case scenarios. But I read John's response and I really like that, so I think we should …

Dixie Baker, MS, PhD _ Senior Partner, Martin, Blanck and Associates
John, why don't you go over your response.

John Moehrke – GE Healthcare
Well, you know, I've got to quick reconnect myself to it. So, yeah, you know, one, I think that we've talked about this on earlier ones about just the recognition of modularity and sometimes third party software is needed. For example, here, authentication is a very common third party, but you really need to do the acceptance of a third party authentication service through some defined interoperability standard. That makes it pluggable so things such as PKI or LDAP or Kerberos or SAML or O-Auth. And I think there is also certifying bodies such as Direct, in the case of certifications, in the case of things like SAML assertions; you see them in the exchange specifications. There are also some positives here in that we have already got some stuff in MU2 that just isn't recognized.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Okay, so, yeah, John's response, I see…I wish I could keep all this up at once. I see down there that Peter you had a comment as well. Are you there?

Peter N. Kaufman, MD – DrFirst – Chief Medical Officer and Vice President, Physician IT Services
I am, but of course it's just now coming up on my screen, because I read other people's comments but I skipped mine when I was preparing for this meeting. This was – what I was talking about was, you know, as we mentioned earlier about the identity proofing levels for a physician with medication being NIST level 3, but that perhaps at some point moving forward, and I think thinking about it now will help everybody in the future, would be to think about eventually having everybody identity proofed that accesses these systems. It is a NIST level 4, which means that everybody accessing the system has two-factor authentication. If you don't have the two-factor authentication, you can't access the system. I'm not talking about identity proofing, but I'm talking about the level of security in the system. A NIST level 3 is just that you have the two-factor authentication for encrypting your entry to the system. But picture a system where different requirements would be for different levels of security. For example, nurses, a nurse's aide probably wouldn't require two-factor authentication identity proofed at level 3, but they might require a level 2 identity proofing, in terms of being able to have that. But being able to share it, so if you worked for a temporary agency, you wouldn't have a credential for each hospital you went to, you'd have one credential that could be shared across the different hospitals, would make it a much more scalable system. But then each of the systems would require a certain level of authentication, and you'd have more trust in the system and less likelihood for at least unpunished data exposure.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Well, we're not talking at all about identity proofing, which is on the operational side, we're really talking about – this question is about certification of products, and the question is, should ONC permit certification of an EHR product as a stand-alone and/or along with third party authentication service provider. So, we're just talking about authentication and certification, we're not talking about identity proofing.

Peter N. Kaufman, MD – DrFirst – Chief Medical Officer and Vice President, Physician IT Services
Right, but you can't separate identity proofing from authentication. Authentication is saying, I'm authenticating that this is the person who they say they are; you're authenticating somebody who was identity proofed at a level 1, that doesn't mean anything.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yeah, but on certification, that's what they do. They have to assume that, you know, we build a system that uses level 3 authentication mechanisms, two-factor mechanisms, they have to assume that the people to whom those credentials were given were sufficiently identity proofed. But when you certify product, you don't certify the process for identity proofing, you just certify …

M
I think the answer…

Peter N. Kaufman, MD – DrFirst – Chief Medical Officer and Vice President, Physician IT Services
If that's the case, then we're getting back to the previous question where third party is probably going to be used more than not third party for these things, especially for this authentication, and we have to say that that's okay.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
Exactly. So I think the bottom line is, you know, like you say Peter, either it should be allowed, and we're all saying that I think is just both should be allowed and then John's point of recognizing more strongly, more specifically the third party software, because that's probably the most likely mechanism that will be used for this type of process.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yeah, and that's the Direct trust is a perfect example of that.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
Yeah.

John Moehrke – GE Healthcare
You know, even something like Microsoft Active Directory is an example of that. If I certify my EHR technology using Microsoft Active Directory, using a standardized interface like Kerberos and LDAP, but you, in your operational environment, chose to use Novell's LDAP directory instead of Microsoft's, are you no longer using certified technology?

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Right, you're not.

John Moehrke – GE Healthcare
Yet, you know, there's really no functional difference because the interface between the EHR proper and the Microsoft Active directory was through a standardized interface. How did Microsoft now become part of this marriage? Well, it was because of the way that MU certification happens today. That was also part of what was in there, in addition to things like Direct Trust as an identity provider.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
You know, all of a sudden, hearing you and Peter back to back here, I'm not sure, is this question asking about using a third party authentication product, which is what John's response is about, and I think Peter's response is about using – yeah, I see what you're talking about Peter. You're talking about using a service where the third party is involved in the authentication. Is that right Peter?

Peter N. Kaufman, MD – DrFirst – Chief Medical Officer and Vice President, Physician IT Services
Yes, it might be a product or it might be a sub-product.

John Moehrke – GE Healthcare
I think Dixie it could be any of those gradients between those, that's what I was reacting to in mine. But, it could be as simple as software, active directory was used, and it could be as big as an identity provider, that is, Verizon's approved identity provider as part of DirectTrust.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yeah. Or it could be a service that calls back your cell phone, you know.

John Moehrke – GE Healthcare
Uh, sure.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
You know what I mean; it could be a service…

John Moehrke – GE Healthcare
Yeah, RSA, right?

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yeah, that actually calls, or they have a lot of these that call back their cell phone and give them a key to enter the system that aren't tightly integrated with the product.

John Moehrke – GE Healthcare
Yup.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yeah. So it's hard to account for all of those. I think, I think both of you have said, what Peter's articulated there, either should be allowed so long as standards are followed.

Peter N. Kaufman, MD – DrFirst – Chief Medical Officer and Vice President, Physician IT Services
Yes.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yup, I think that that's – yeah, we need to converge both of your comments together, but I think the two together is what we want to so.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
Um hmm.

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
Yeah, that's clearly the…

Leslie Kelly Hall – Healthwise – Senior Vice President
As we raised this point earlier about being compatible with NSTIC and that compatibility means that we would adhere and approve to that, even though it wasn't considered EHR technology.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yeah. Yeah. Well, they say …

John Moehrke – GE Healthcare
That's what should be encouraged, right, I mean, honestly …

Leslie Kelly Hall – Healthwise – Senior Vice President
Absolutely.

John Moehrke – GE Healthcare
The last thing we want to do is have, you know, the software developers who are great at clinical decision support and all kinds of medical algorithms, inventing security algorithms. You don't want that.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Wall, what if they used, going back to the NSTIC question, how about if this third party authentication product had actually been certified by a different entity that certifies security products? Should it get special points for having been certified?

Leslie Kelly Hall – Healthwise – Senior Vice President
I think it should be either/or, either meeting the EHR certification, as defined, or, at the NSTIC level 3, or whichever NSTIC equivalent that we've said complimentary.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yeah, that's a NIST level 3; the NSTIC is what follows it.

John Moehrke – GE Healthcare
Yeah, I think Dixie you were actually opening it up to recognized certifying technology…

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Certified…

John Moehrke – GE Healthcare
Yeah, because like LDAP and Kerberos are indeed certified by …

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yeah, yeah, they have common criteria certification, they have … yeah.

John Moehrke – GE Healthcare
Again, I think that works great for large organizations, I think being able to prove that certification for a small organization might be pretty onerous.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
You don't mean product certification, it's not organiz …

John Moehrke – GE Healthcare
Yeah.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Oh, you mean the small vendor, yeah, yeah, they are onerous, yeah, that's a good point. So what we want to capture here Charlie is that yes they should be allowed and in fact encouraged. And we will combine the good poin – the points that both John and Peter made on this one. This is going to be a long answer for us, but we have a lot of good stuff here, so I don't think…so, we'll go back and just try to combine them so that we don't repeat ourselves. But, we'll combine them. Okay? All right. Let's go on to the next one. Good discussion. Good.

Okay. This one is, what if any security risk issues should be subject to meaningful use attestation in Stage 3. For example, the requirement to make staff work force aware of HIPAA Security Rule and train them on security rule provisions is one of the top five areas of Security Rule noncompliance identified by the…what they're trying to get to is…are HIPAA requirements that if not followed raise the greatest risk. And they use the example of work force awareness, you know, staff training is another one where if not followed, they really bring a lot of risk to the organization and, so that's what they're asking about. What are the HIPAA requirements that if not followed, raise the greatest risks in an organization?

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
Well, an so my answer was, there are 42 implementation specifications in the HIPAA Security and my sense is, they are what they are and I don't think they should be put into this process of getting incorporated somehow into the detail level of meaningful use. I think that a lot of them are certainly internal operational and workflow activities that people follow based on the risk assessment and the reasonable and appropriate level of implementation and all that and so, trying to make them be part of meaningful use would begin to micromanage to a level that I think would be inappropriate to handle. And if there was anything that needed to be done, it would be done not by meaningful use, but by OCR through compliance. So, my answer basically is, I don't think there's any reason for or need to detail specific implementation specifications of HIPAA Security as part of meaningful use, in terms of an attestation or some other way of demonstrating meeting those.

M
I agree.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
And John?

John Moehrke – GE Healthcare
Yeah, I basically agree. I did have the other little comment that, a HIPAA violation should maybe be seen as against, you know, their certification, but I don't think they should extract anything out of HIPAA and add it to attestation.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Well they, first of all, OCR doesn't disclose that, so that's not visible. But I happen to thin –I think there are certain, you know, I'm kind of ambivalent about this because on the one had you don't want to target any particular HIPAA requirement and say, well that's more important than others. But I think there are things that are more important like, that really change the culture, you know, like staff training, like reminders, like, you know, that engender the culture of security within an organization. So, that's what my response was all about. You know maybe consider those. I mean, we know from surveys, the HIMSS surveys for example, that most people don't even do the risk assessment. So …

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
What's interesting, Dixie is that by creating this level of requirement on one of the three types of covered entities under HIPAA, the other two don't have to do anything.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
What are you talking about?

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
Well, I'm talking about providers, those are the ones that are subject to meaningful use…

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Oh yeah, that's a good point. You mean versus clearinghouses …

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
… versus clearinghouses and payers. Now payers have now a new compliance certification coming up, but the compliance certification relates mostly to the HIPAA transactions and … and operating rules and standards around that. So, it would create a, you know, different level of expectation, you know, providers having to attest that they do training whereas clearinghouses don't have to attest anything.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
But the risk is highest there too. The risk is way higher in the provider than in clearinghouses and payers. They have much more data …

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
Ohh, I don't know. But, in any case, I think …

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Okay, so do I hear consensus that we should just say there should be none called out basically? Yes.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
Yes, I agree with that.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Okay. Right. So, we'll just go with Walter's comment there, go with Walter's comment, that's the one we'll throw forward. Okay. Next question. Ah, are we at the end, oh no…

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
No, we have 05, 06, 07.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Oh, okay.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
05 is it feasible to certify the compliance of EHRs based on the prescribed standard.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
I think we need to see something above that maybe, let's see …

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
Oh, well …

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yeah, there's feedback on standards for accounting for disclosures, would also be appreciated.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
Yes, that's right.

John Moehrke – GE Healthcare
Ah yeah, this is the E-2147.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
Yeah.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
And then I made a comment here that these questions that follow are confusing because this introductory paragraph is asking for feedback on accounting for disclosures, and then, we switch to topics … then switch it to the topic of audit reports and – and I think this is important to point out, that audit logs capture activities within the system, but they don't capture all of those elements that are needed to account for all disclosures.

John Moehrke – GE Healthcare
Exactly.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
In fact, that ASTM standard that they cited for audit, for accounting the disclosures, even addresses the two separately. So, these are really odd questions, I think.

John Moehrke – GE Healthcare
Well, I think it's an opportunity for us to educate, because this is a common misunderstanding.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
Um hmm.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
But these questions, it sounds like they relate all to audit, not accounting of disclosures.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
I think they were trying to get to accounting of disclosures and then they use the audit as a way of achieving accounting of disclosures.

John Moehrke – GE Healthcare
You know, that's closer to an access log.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
Yeah, oh, exactly.

John Moehrke – GE Healthcare
You know, which is that NPRM that kind of has just stopped.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yeah.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
Yeah.

John Moehrke – GE Healthcare
It's far easier to do an access log based on the ASTM E-2147 because indeed it is very supportive of that.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Well, ASTM E…

John Moehrke – GE Healthcare
But I think when you get to asking the question Dixie, we're all pretty aligned. Yes, you can. It is a functional specification, you can test to it.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yes.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
But then the other part of the answer is your, both of your points, Dixie and John, about ASTM E-2147 is not as specific or the one to expect to use for accounting of disclosures.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yes it is. It has two separate lists in it. It has one list of the data elements required in an audit log and it has a separate list of data elements to be captured in a disclosure log. So the answer still is yes. I think my answer there is the answer we should use there, because it does point out that they are two separate things, but all of us agree that it can be tested.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
Well, okay, I guess assuming that the accounting of disclosures is really about disclosure, they're not active reports.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
It is, it is. The list in ASTM 2147 is clearly a list of accounting for, accounting of disclosures, it's not a list for, they have a totally separate list for…

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
Well yeah, no, the point is, today "accounting of disclosures" under the proposed rules is not a, is don't disclosures is access.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Now they have two separate … in that NPRM had two separate reports, they created a whole new report for an access report that was internal. That was a whole separate thing. And then they also had separate requirements for accounting of disclosures between organizations. They just added something to it.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
I'm fine going with, you know …

John Moehrke – GE Healthcare
Yeah, I think the issue there though is, it's less about the data elements that need to be captured and more about what has the ability to capture, because disclosures tend not to be known by the EHR technology.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yeah they aren't – yeah, that's …

John Moehrke – GE Healthcare
I mean, that's the biggest problem with an accounting of disclosures is, it tends to be those things that happen outside of the workflows that the EHR operate off of. EHRs tend to operate off of completely the exception, which is CPO.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Well, they define EHR technology so broadly, in fact, I once asked the specific question about interface engines, which do know a lot about disclosures and they said, oh yeah, that's EHR technology. So, if you define EHR technology as including your entire network and your interface engines and everything in a provider organization, yeah, EHR technology has that knowledge. But, if you're really looking at CPOE, no, it doesn't know that knowledge. But maybe we should add that point, that the … included in the disclosure log, but make the point that, you know, stress that we're talking about disclosures between organizations, just to be real, real clear. That's – yeah, that's a good point, a good idea. Okay, let's go on, we need to – is everybody still there?

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
Yeah…

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Oh, look at this one. I love these an … is it appropriate to require attestation by meaningful users that such logs are created and maintained for a specific period of time? I like Walter's answer, that's good. It looks like all of us do. Oh, okay. We do have more comment. Okay, Peter and John, let's hear your thoughts.

John Moehrke – GE Healthcare
Yeah, I think I'm just more verbose on this, but I'm kind of wondering why is this being explicitly pulled out as an attestation requirement.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Versus other HIPAA requirements, yeah.

John Moehrke – GE Healthcare
Yeah.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yeah, it's the same answer as before, I guess.

John Moehrke – GE Healthcare
Yup.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yeah, and Peter?

Peter N. Kaufman, MD – DrFirst – Chief Medical Officer and Vice President, Physician IT Services
I'm just concerned about adding that kind of time or staff requirement for logging this kind of thing. You know, everything has value, but it's all about risks and benefits or benefits versus cost. Cost and benefits and in this case, it looks like the cost is going to be high for the practice. Just trying to protect my friends out there practicing.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Well are you talking…well, we're not being asked about the complexity of the log, because that's already law. The accounting of disclosures is already in the law, we aren't being asked about that. What we're being asked about is whether as part of meaningful use, they should be asked are you complying with that law or aren't you.

Peter N. Kaufman, MD – DrFirst – Chief Medical Officer and Vice President, Physician IT Services
Ah, well, I misunderstood. If it's a law, then it shouldn't be required for meaningful use.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yeah, it seems like a question very similar to the HIPAA one.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
I think, I would like to change my response then, to yes, I agree. I think this is one of those, yeah, HIPAA elements and I'm …

John Moehrke – GE Healthcare
Yeah, the problem – so here's an example of potential problem, and I don't think it's worthy of too much discussion, but, you are required to be able to produce an accounting of disclosures for the previous seven years, right?

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
Upon request.

John Moehrke – GE Healthcare
But that does not mean that you have the whole E-2147 audit log back seven years; it just means that you can produce an accounting of disclosures for a particular patient. And, you've got lots of time to produce that. So, you might be going through off-site technologies, you might be using annual reports…

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Yeah, you're able to come up with it.

John Moehrke – GE Healthcare
Yeah, and so you're able to meet the HIPAA requirement. But this here is saying, not only do you have to create … meet the HIPAA requirement, but you have to maintain the whole ASTM 2147 requirement for seven years.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Why don't we make this response the same as we did the … one?

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
I agree. I think that's – I like that.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
And Walter, you – I had told Walter beforehand, I have an appointment I need to be at in fifteen minutes, so Walter would you lead the discussion of the final question here.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
Sure, yeah, absolutely.

Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner
Oh, I see there are two more, but …

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
I think it's two more, yeah.

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck and Associate
We'll get these, our comments together later on today. Thank – okay, thank you.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
Thanks Dixie. So, we're moving to 07. Is there a requirement for a standard format for the log files of EHR to support analysis of access to health information across, I suppose, multiple EHRs or other clinical systems in a healthcare enterprise? So, is there a requirement for a standard format for the log; it does make sense. So my response was while having a standard format for the log files would be beneficial to facilitate the analysis of access to health information, the requirement should focus on the ability of EHRs to produce the necessary information to support that analysis, not necessarily the format of the files. So in other words, conceptually the requirement should not be the format of the files, but a requirement that says that the EHR is capable of producing the information that is needed to do the analysis of access to health information. And I see there's – John, do you want to talk a little bit about your response?

John Moehrke – GE Healthcare
Well, I'll first start with, I think you have a nice succinct one there, and that's essentially all I say. You know, I do point out that ATNA is often times pointed at, but it's not a file format, it's a way…it's an interoperability spec for how to move the audit logs in real time to a service. So, it's a service-oriented architecture, so I would like to support a service-oriented architecture, again, this gets to some of the other discussions we've had. But I think your comment is sufficient.

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
So John and Walter, this is David. Could I ask a question?

John Moehrke – Interoperability & Security _ GE – Principal Engineer
Sure.

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
It is not a space that I have thought a whole lot about, but it seems to me that we heard testimony way back at the beginning of the privacy and security work in the first stage of meaningful use about the difficulty of detecting breaches and other inappropriate access when the security logs were spread out all over the place and were in different kinds of formats, and that a lot of work was required on behalf of the providers to reassemble a time sequence trail, if you would, of access through a system. And I remember coming away from that with the impression that we could do some good if we did standardize those formats to make that process easier to do. Is that just not feasible? Is that too much work?

John Moehrke – GE Healthcare
Well I think in a large organization, it's very reasonable to utilize something like a service oriented architecture to centralize your security audit logs, and that's what IHE-ATNA is focused on doing. The problem being, how do you mandate that and support small organizations that don't need that? And that has always been the reason why ATNA gets kicked out, is that it is unnecessary and possibly burdensome for technology that's intended to go into a small organization. Now, I don't …

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
Does that mean that ATNA may be the wrong standard, is that just too complicated?

John Moehrke – GE Healthcare
No, no, no. I don't think so. I think the problem is that in a small organization, you have a single piece of technology, you don't have multiple pieces of technology doing your work, so the analysis of a single system is, the single system does the analysis. It's only when you get into large organizations that have very distributed EHR that you need that.

Mike Davis – Veterans Administration
I think John, that in either case, it's useful to have a standardized listing of information that must be collected by the audit system in order to meet your reporting requirements, if you're using it for such things. If you don't have the data elements in the system, then you can't collect it and so the larger systems, that's absolutely correct, there are multiple formats of the audit trail, but, in a service oriented thing, they're going to attempt to harmonize those for reporting and statistical analysis, etcetera, into a common format. And that's the other issue there, to ensure all these different sources are at least collecting the data elements that you need. So I think – I mean, if you looked at ATNA not as a specification to implement as a service, but as information that supports healthcare audit, then that is quite useful.

Just to Dixie's point here, which I don't entirely agree with, she says there's no requirement for a centralized enterprise thing. But, I think there's a requirement that we be able to provide to the patient listings of who has seen their records, and that is typically not collected in an audit trail. Typically, you collect the name of the user, the tables and stuff that they, the database that they access. But the name of the user is only specified like in ATNA, to specifically have that kind of element. So … the kinds of things that you need to collect, I think it's useful.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
So Mike, just to maybe a clarification point, you said we're required to – the patient who accessed their record. I think at this point at least, we're required to provide the patient who did we disclose the data to, not necessarily who accessed the record. That's the big difference between account of disclosures versus an access report that was in the proposed rule. So, now in terms of being able…this use of the work access to health information, in other words, is somewhat looking at if an entity has to do an internal analysis to know who accessed the health information, for whatever purpose, for a breach analysis or some other reason. Is there any benefit of having a standard format of the logs, that the standard format of the logs are beneficial in many respects for interoperability? In other words, for, I mean, the standards were when you have to exchange data, right, I mean, in other words, you're going to send out data and so in order to have the entity that receives the data be able to receive it and process it, you need to have the standard.

Mike Davis – Veterans Administration
I don't think it's limited to that. A lot of … our EHR systems have what you … an EHR component, we have components for imaging, they are separate systems, right. So if we're doing auditing, and there are many separate systems that go together to make what we would call an EHR. So, it's necessary to harmonize and collect that information together and …

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
Yeah, that's…

Mike Davis – Veterans Administration
… you cannot specify how an operating system, they're designed. They're going to do whatever they're doing. So…

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
So you're saying, yeah, internally there's also a need for internal interoperability.

Mike Davis – Veterans Administration
Right. You need to be able to collect data from diverse sources and bring it up to a common level for analysis and understanding, you don't want to … right, so I think that's possible.

John Moehrke – GE Healthcare
So I think the question is, and this is actually tied to the next question, so I think by discussing it, we're hitting both. I think that the question becomes, is there a way that we can help deal with the scalability issue, i.e. technology that's intended for a small scale, to meet functionally the ASTM specification may be all that's necessary. But, any system that goes into anything other than a small organization would absolutely benefit by being capable of doing IHE-ATNA.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
Yeah, so we're saying, it is beneficial to have a common set of data elements, first of all, and then a common format, because those are two separate things, common format for maintaining the logs.

John Moehrke – GE Healthcare
The data elements are already in play, I mean, that was the specification in MU2 under ASTM 2147, that's the common data elements and the common events, I mean, were listed there.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
So then the concern is the scalability.

John Moehrke – GE Healthcare
Yeah. I mean, I think your comments on log format are on and I think that the question of using ATNA isn't a log format; it is a way to deal with scalability when you have many systems that are used to access the health information. So, I just – if we can come up with some way to deal with the scalability, I would feel happier.

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
But, do we like Mike's suggestion that the ATNA is a good … for the data that should actually be captured, even if we don't specify an exact format?

John Moehrke – GE Healthcare
I don't think that's right. I think the ASTM E-2147 has already done that. I mean, that is indeed the core functional specification that ATNA is based on.

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
Right, so that's – why is this – I naively thought that this was already covered by ATNA, but when Mike raised the point, I realized maybe it's not.

Mike Davis – Veterans Administration
Well my point is 2147 is in ATNA. My point is more to the service oriented nature of consolidated, multiple audit formats, not to try to force 2147 on every data-collecting unit as a specification, right. To harmonize audits to something like, you know, 2147, in a service that's responsibility is to coordinate across these diverse audit systems. So, I think that's my point, it is an important point for a lot of organizations that have multiple components in their EHR. It's…

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
So, to answer then – I mean, for 07, we're saying there is, again, I think we have the answer that there is a, having a standard format for log files would be beneficial, but, I mean, we all argue that the important part is the what and not the how, although they…

John Moehrke – GE Healthcare
Right.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
Yeah.

Mike Davis – Veterans Administration
So, I just want to be careful we don't stay a standard format for log files being a specification that all end-points have to adhere to. There has to be, it would be nice to be mapable into a standard format. This is what I've done in the past in audit systems, I've done this for … scale DOD systems. You know, you map the diverse audit trails of individual components into a common format so that you can have some sanity, you know, at the end.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
So we can add that point, that it would be valuable to have the data be mapable to a common format.

Leslie Kelly Hall – Healthwise – Senior Vice President
This is Leslie and, is it – I think we're not having the tail wag the dog, because if there's going to be standards for log files, I don't think that is as important as standards for the … use and for security and privacy interoperability among systems. So, if this can help drive that, great, but if this becomes just a burden, then I think it's difficult.

Mike Davis – Veterans Administration
Well it kind of works both ways. You can't – if you're trying to get interoperability, you have to do it inside of your own organization with the audit sources that you have before you can talk about exchanging information with somebody else.

Leslie Kelly Hall – Healthwise – Senior Vice President
Okay.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
So, and then to, so, we have, I think, a good answer for this and for 08, are there any specifications for audit log formats that are currently widespread? We provide, actually all of us have provided several examples there, so we can just use those and that's simply the answer basically, we don't need to…we just need to provide which are the examples. Any comments on 08?

John Moehrke – GE Healthcare
The only other comment I can bring up is, back when I was part of the kick-off of CCHIT, we somewhat answered this by saying yeah, let's require that they can export them into a structured text file format of undefined format. Because as soon you can export the log files in text, you can probably do all this mapping that Mike is bringing up. But if you don't have the ability to export into a text file, you don't have the ability to do the mapping. And I hate to go back to that as the low bar.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
Yeah, that's a good way to go – to being able to map it, if you can put it out in a text format, but …

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
The double CSV for everyone, right?

John Moehrke – GE Healthcare
Yeah, exactly. It's a structured format, but not defined.

David McCallie, Jr., MD – Cerner Corporation – Vice President, Medical Informatics
I think in our language here we need to be careful to distinguish between data elements and this notion of, this vague word format or layout. I can't read all the words on the screen, but, make sure we're not talking about standardizing data elements when we say format and vice versa.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
Yes, exactly. That's the point I think we're getting to in the previous question, is, there's a value of having common data element set which is ASTM and then a common format, both of them. So, yeah, good point. All right, I think we have like three more minutes to go and we should probably then let the call be opened for public comments. MacKenzie, can we open it for public comments?

MacKenzie Robertson – Office of the National Coordinator
Sure. Hi, operator, can you please open the line for public comment?

Caitlin Collins – Altarum Institute
Yes. If you are on the phone and would like to make a public comment please press *1 at this time. If you are listening via your computer speakers, you may dial 1-877-705-2976 and press *1 to be placed in the comment queue. We do not have any comments at this time.

Walter Suarez, MD, MPH – Kaiser Permanente – Director, Health IT Strategy & Policy
Okay. All right. Well, I know Dixie would have wanted to say this, but, on behalf of her and myself, thank you everyone for participating in this marathonic review of all these questions. What we will do is we will wrap up the document later this afternoon and send it out to everyone, just to make sure that it looks okay and then we will be sending that to ONC, I think still the deadline we want to meet is Monday, which is the deadline for the Policy Committee comments. So, that's what we will do and again, thank you so much for participating in this process and we will, with Dixie, look at what's next in our agenda and then bring back the group into a future call for addressing whatever we have next in our agenda. But for now, I think this really concludes our priority work on the comment process and so look forward to our meeting of the full committee later this month and thanks so much again and have a great weekend.

M
Thank you Walter.

MacKenzie Robertson – Office of the National Coordinator
Thanks everybody.

Leslie Kelly Hall – Healthwise – Senior Vice President
Thank you.